WATERMARKING USING WAVELET AND SINGULAR DOMAIN WITH DIFFERENT DUAL SCRAMBLING METHODOLOGY

Shweta Bhati[1], Heena Joshi[2], Komal Sharma[3],Vandana Matai[4]

[1,2,3,4]Asst. Professor, Dept. of ECE Engg., J.I.E.T., Jodhpur, Rajasthan, India

Abstract

The method used in this paper fully exploits the features of DWT and SVD transform domains by implementing on several images having different texture, contents and different magnitudes of singular values along with the images of different file formats like bmp, tif, png, gif and jpeg. Dual scrambling methodology having different characteristics is implemented resulting in the high level of security. The appropriate scaling factor/embedding factor is also judged from a fairly wide range of values from 0.01 to 0.09.Various degrees of scrambling and histograms are also presented with different images that can be applied with the proposed method. A comparison with the two previously proposed algorithms is made.

Keywords: DWT, SVD, PSNR, NC, BER, MSE

I INTRODUCTION

Gradual development of digital multimedia content publishing technology has improved the ease of access to digital information. Digitizing of multimedia data has made reliable, faster and efficient storage, transfer and processing of digital data. It also leads to the consequence of illegal production and transmission of duplicate and modified digital media which has become very easy and undetectable. So, Watermarking is adding "ownership" information in multimedia contents to prove the authenticity. This digital watermark can be detected or extracted later to prove the authenticity of the data. The embedded watermark should be imperceptible and robust enough to survive both common signal distortion as well as distortions caused by malicious attacks. On the modification of any data content, could lead to absence or degradation of the watermark.

II WORKING DETAIL

In most of the research work done, the watermark is scrambled before the embedding procedure and is generally a binary message of small size as a watermark [4]. This study proposed a technique using dual scrambling method in wavelet and singular domain for embedding and extraction of a digital image watermark. In this method the host image is scrambled using another scrambling sequence before the watermark is inserted. The host image is first scrambled and decomposed into multi-resolution sub-bands using three levels DWT. The image decomposition is done with "Haar" which is a symmetric, simple and orthogonal wavelet. The SVD is then applied to a selected sub band. This results in three matrices U, S and V. The dual scrambled watermark using Arnold scrambling and scrambling sequence is then inserted by modifying the singular values of matrix S in an image.

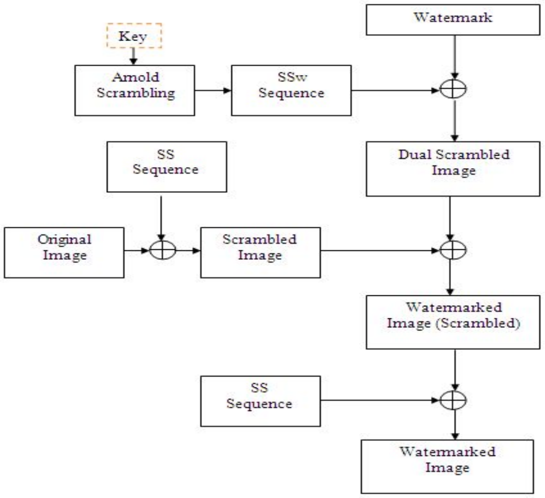


Fig 1. Embedding after Scrambling

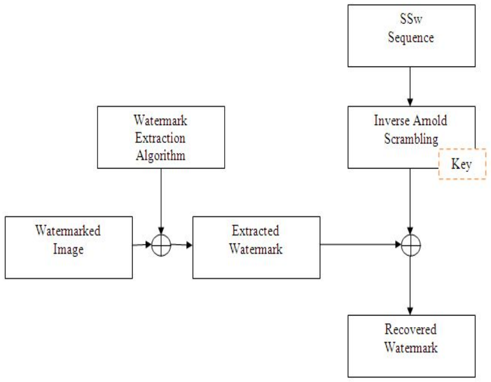


Fig 2. Extraction after Scrambling

III PARAMETERS

a) Imperceptibility

Imperceptibility means that the perceived quality of the cover image should not be distorted by the presence of the watermark. As a quantitative measure, Mean Square Error (MSE) and PSNR metrics are used [3].

Mean Square Error (MSE)

Mean Square Error between original image and watermarked image is calculated as follows:

$$MSE = \sum_{i=0}^{n-1}\sum_{j=0}^{m-1}((a_{i,j} - b_{i,j})^2)/(n*m)$$

Where m × n is the image size, $a_{i,j}$ and $b_{i,j}$ are the corresponding pixel values of two images.

Peak Signal to Noise Ratio (PSNR)

PSNR is calculated between the original and the watermarked image. Larger the PSNR value, more similar is watermarked image to the original image. This image quality metric is defined in decibels as:

$$PSNR = 10\ \log_{10}(\frac{255}{MSE})^2\ \ dB$$

b) Robustness: Robustness means measurement of the immunity of the watermark against stabs to remove or degrade it, intentionally or unintentionally, by different types of digital signal processing attacks.

Normalized Correlation (NC)

If the extracted watermark image is absolutely tally with the origin watermark image, the Normalized Correlation (NC) =1. Otherwise the NC is between 0 and 1. When the extracted watermark image is more tally with the origin watermark image, the NC is bigger(Singh, Choudhary and Agrawal, 2011).

$$NC = \frac{\sum_{i=0}^{N}\sum_{j=0}^{M} W(i,j) * W^*(i.j))}{\sum_{i=0}^{N}\sum_{j=0}^{M}[W(i,j)]^2}$$

Where,

W (i, j) = Original watermark image

W*(i, j) = Extracted watermark image

N and M = Width and height of the watermark image

Bit Error Rate (BER)

Bit error rate refers to the amount of watermark data that may be uncorrectly embedded within a host signal per unit of time or space, such as error bits per second or error bits per pixel. For the cover image and watermarked image of length L bits, the BER (in percent) is given by the expression:

$$\mathrm{BER} = \frac{100}{\mathrm{L}}\sum_{\mathrm{n}=0}^{\mathrm{L}-1}\begin{cases}1, & \check{\mathrm{c}}(\mathrm{n}) \neq \mathrm{c}(\mathrm{n})\\ 0, & \check{\mathrm{c}}(\mathrm{n}) = \mathrm{c}(\mathrm{n})\end{cases}$$

Robustness to Image Processing Operations

Watermarked digital images may undergo common signal processing operations such as salt & pepper, various filtering methods, cropping and histogram equalization. The histograms of the various cover images and their corresponding watermarked images are shown in fig 4.6 to represent the intensity transform of the images so that the gray levels in the input image maps to the gray levels in the output image.

c) Computational Complexity

Computational complexity refers to the processing time required to embed the watermark data in the original data, and / or to extract the data from the original data. The elapsed time or processing time of the CPU (in seconds) to embed the watermark is computed in order to measure the computational time of the proposed algorithm.

IV. RESULT

The proposed algorithm is tested on various different grey scale images of size 512 x 512 with different formats like bmp, tif, png, gif, jpg, etc.

The JPEG compression is a lossy compression and its compression rate depends on the quantization level used. Quantization eliminates the high frequency data that contains image details, noise and embedded watermark. Hence, higher compression ratio corresponds to lower image fidelity. Various filters are normally used for eliminating noise in the images. Geometric attacks consider the image as a geometric object such as a square or rectangle and apply simple geometric transforms which are not perceptible by the viewer. Rotation does not destroy the visual content of an image but move some pixels to new positions along with some pixels of the embedded watermark. Cropping attack refers to the cutting of some of the significant part of an image. Also the histogram equalization distributes the intensity of the pixels evenly throughout an image. table 1 summarizes the results of applying different attacks to the cover image “dollar” having .bmp file format.

Table 1. The watermarked images after certain attacks on dollar image

Original Image	Salt & Pepper(0.01)	Salt & Pepper(0.02)	Salt & Pepper(0.03)
Image 1	Image 1	Image 1	Image 1
PSNR: 64.4849 MSE:12.0021 NC : 0.9806	PSNR: 30.8958 MSE :23.2726 NC :0.9949	PSNR: 27.8598 MSE :26.2446 NC :0.9909	PSNR: 26.1731 MSE :26.1731 NC :0.9979
Salt & Pepper(0.04)	JPEG(30)	JPEG(40)	JPEG(50)
Image 1	Image 1	Image 1	Image 1
PSNR: 24.9050 MSE: 29.2634 NC : 0.9835	PSNR: 30.8189 MSE :23.3495 NC :0.9971	PSNR :32.0142 MSE :22.1542 NC :0.9964	PSNR :33.0592 MSE :21.1093 NC :0.9940

The same attacks are also applied to the “lighthouse” standard test image having .png file format in Table 2..

Table 2. The watermarked images after certain attacks on lighthouse image

Original Image	Salt & Pepper(0.01)	Salt & Pepper(0.02)	Salt & Pepper(0.03)
Image 2	Image 2	Image 2	Image 2
PSNR :63.4545 MSE:-9.2861 NC :0.9849	PSNR :31.2552 MSE :22.9132 NC :0.9944	PSNR :28.3837 MSE :25.7847 NC :0.9977	PSNR :26.1731 MSE :26.1737 NC :0.9985
Salt & Pepper(0.04)	JPEG(30)	JPEG(40)	JPEG(50)
Image 2	Image 2	Image 2	Image 2
PSNR :25.2746 MSE :28.8938 NC :0.9996	PSNR :36.2091 MSE :17.9514 NC :0.9922	PSNR :37.7603 MSE :16.4081 NC :0.9918	PSNR :38.4268 MSE :15.5684 NC :0.9892

To show the applicability of the proposed algorithm , table 3. summarizes the results of these attacks on the “woman” image having .tif file extension.

Table 3. The watermarked images after certain attacks on woman image

Original Image	Salt & Pepper(0.01)	Salt & Pepper(0.02)	Salt & Pepper(0.03)
Image 3	Image 3	Image 3	Image 3
PSNR :59.2816 MSE :-5.1132 NC :0.9804	PSNR :31.5228 MSE :22.6457 NC :0.9937	PSNR :28.5837 MSE :15.5847 NC :0.9910	PSNR :26.6731 MSE :26.1731 NC :0.9867
Salt & Pepper(0.04)	JPEG(30)	JPEG(40)	JPEG(50)
Image 3	Image 3	Image 3	Image 3
PSNR :25.5579 MSE :28.6105 NC :0.9827	PSNR :37.3755 MSE :16.7929 NC :0.9913	PSNR :38.9905 MSE :15.1779 NC :0.9902	PSNR :39.5468 MSE :15.5216 NC :0.9881

The same attacks are also applied to the “lena” standard test image having .gif file format in Table 4.

Table 4. The watermarked images after certain attacks on lena image

Original Image	Salt & Pepper(0.01)	Salt & Pepper(0.02)	Salt & Pepper(0.03)
Image 4	Image 4	Image 4	Image 4
PSNR :69.9820 MSE :-15.5520 NC :0.9887	PSNR :31.5109 MSE :22.6575 NC :0.9952	PSNR :28.3837 MSE :25.7847 NC :0.9946	PSNR :27.8598 MSE :26.1731 NC :0.9910
Salt & Pepper(0.04)	JPEG(30)	JPEG(40)	JPEG(50)
Image 4	Image 4	Image 4	Image 4
PSNR :25.4533 MSE :28.7133 NC :0.9822	PSNR :40.3193 MSE :13.8491 NC :0.9966	PSNR :40.8101 MSE :13.3583 NC :0.9964	PSNR :42.1092 MSE :11.9281 NC :0.9948

The results in the above tables are conducted on the different file formats like bmp, png, tif, gif and jpg of an image keeping the scaling factor constant at 0.02. The results shown above depict the strong robustness of the proposed algorithm under all circumstances.

The extracted watermarks are shown in Table 5. and it can be observed that the proposed scheme can not only successfully resist different kinds of attacks but can also restore watermark with high perceptual quality.

Table 5. Varied Scaling Factors

	Dollar image		Lighthouse image		Woman image	
SF value	PSNR	NC	PSNR	NC	PSNR	NC
0.01	64.1027	0.9764	62.7598	0.9760	59.6742	0.9740
0.03	64.3353	0.9720	62.1795	0.9783	57.4908	0.9752
0.05	62.4180	0.9802	61.6332	0.9811	56.9982	0.9801
0.07	60.9861	0.9859	60.6224	0.9861	56.0468	0.9869
0.09	58.6811	0.9969	59.5535	0.9901	54.1786	0.9938

It can be observed that the larger the scale factor, the stronger the robustness of the applied water marking scheme. In contrast, the smaller the scale factor, the better the image quality. Therefore the value of 0.02 is taken for these set of images which consist of both the properties and gives the best results.

V PERFORMANCE ANALYSIS

a) On the basis of Degree of Scrambling (DOS):

Degree of scrambling can be defined as the number of bits in an image that gets exchanged with its diagonal counterpart. The size of the scrambled sequence is equal to the size of the original image.

In the scrambling methodology, as the degree of scrambling increases, the no. of bit error increases. This increase in the bit error leads to the rise of noise in the signal which finally results in the reduction of the PSNR value. In the proposed strategy the scrambling of the image leads to decrease in its quality but it makes the watermarking more robust.

b) On the basis of JPEG Compression Attack:

The JPEG compression standard is considered as the most significant attack and is a lossy type of compression. Its compression rate depends on the quantization level used where the higher compression ratio corresponds to lower image fidelity. The quantization eliminates the high frequency data that consist of image details, noise and embedded watermark.

Table 6. NC values at different JPEG compression degrees

Compression degree	Image 1	Image 2	Image 3	Image 4
30^0	0.9971	0.9922	0.9913	0.9966
50^0	0.9940	0.9892	0.9881	0.9948
70^0	0.9989	0.9871	0.9865	0.9932
90^0	0.9847	0.9853	0.9807	0.9916

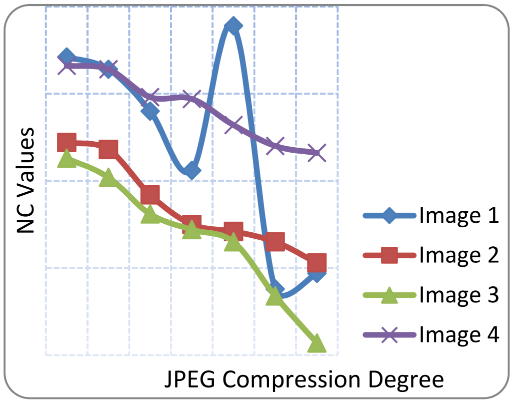


Fig 3. NC values at different JPEG compression degrees

Fig 4. shows the NC values corresponding to the various JPEG compression degrees respectively.

Table 7. PSNR values at different JPEG compression degrees

Compression	Image 1	Image 2	Image 3	Image 4
30^0	30.8189	36.2091	37.3755	40.3193
50^0	33.0592	37.3581	37.9281	42.1092
70^0	35.8600	39.1072	39.6215	43.4266
90^0	43.4266	44.7780	44.8563	46.8516
100^0	61.3280	61.1426	57.8899	64.1078

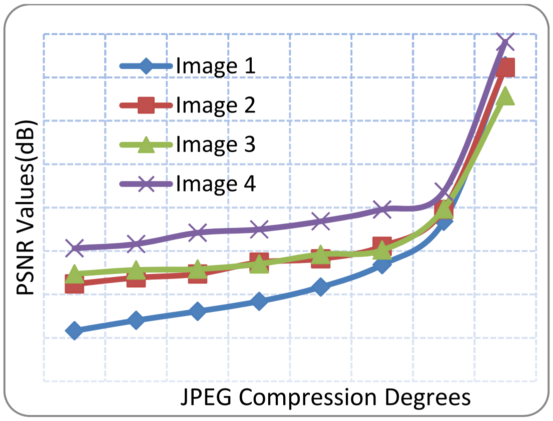


Fig 4. PSNR values at different JPEG compression degrees

Fig 4.4 shows the PSNR values corresponding to the various JPEG compression degrees respectively. The robustness of the proposed method can be clearly observed with the graph as the value of the parameters increase with the increase in the compression degrees. Security is considered as having the most financial implication with a high demand in the commercial market, thereby considering the security as the prime concern.

c) On the basis of Comparison:

We compare the results with [2] using the NC values between the extracted watermark and the original watermark. The results show that the proposed method is more robust than [2] especially on salt and pepper noise, Gaussian noise, JPEG compression and cropping attack.

Table 8. Comparison of various algorithms using NC values

Authors	Salt & pepper noise	Gaussian Noise	JPEG compression	Gaussian low pass	Cutting
Rui-mei *et al.*	0.9284	0.9125	0.9944	0.9875	0.9113
Wang *et al.*	0.9312	0.9502	0.9439	0.9335	0.8286
Proposed method	0.9946	0.9973	0.9964	0.9842	0.9453

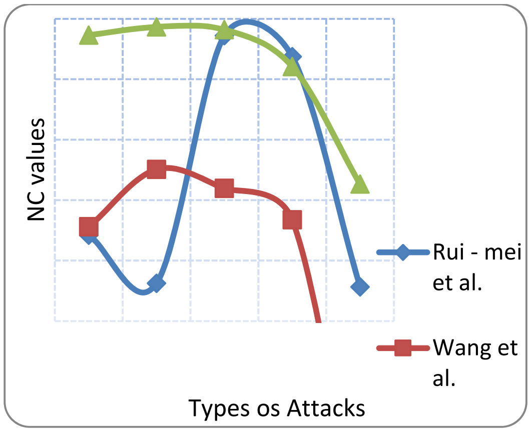


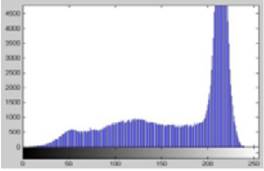
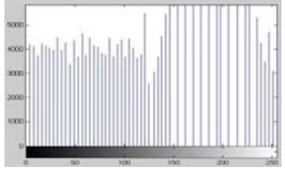
Fig 5. Comparison of various algorithms using NC values

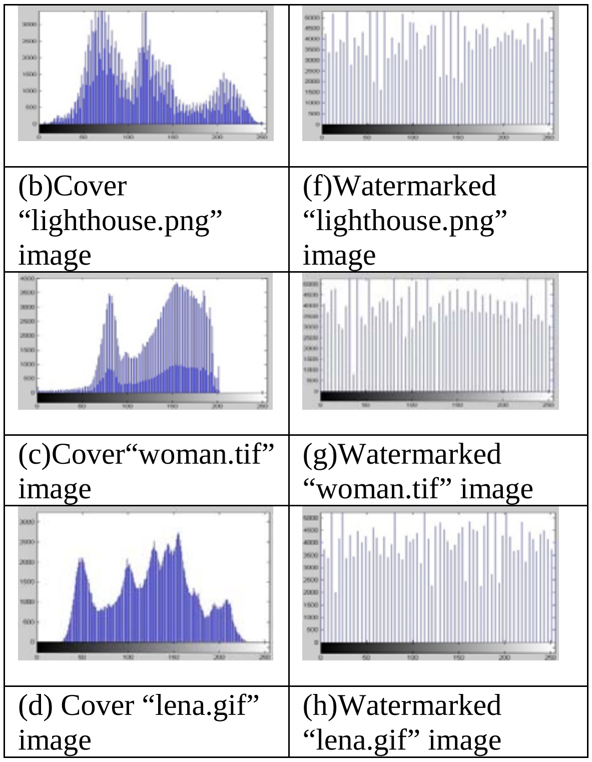
Figure 6. demonstrates the considerable better results of the proposed method than the other two algorithms in the various signal processing operations. Despite the better performance of the proposed watermarking method, there exist some limitations. The NC values are better in the compared results, but the PSNR value slightly decreases. [2] have PSNR values as 42.0326dB and 76.46dB respectively while the proposed method has 69.9820dB. It is due to the introduction of dual scrambling methodology in the watermark and cover image that results in the increase of errors in the number of bit pixels. This leads to the rise of noise in the signal that reduces the PSNR value significantly. The proposed method leads to decrease in its visual quality slightly but it makes the watermarking method more robust. It is due to the fact that the exact location of the watermark insertion cannot be known due to the scrambling of the cover image.

d) On the basis of Histogram Analysis and Computational Complexity:

Image histograms are used as important feature during the analysis of the watermarking method. Each bin in the histogram represents the number of pixels whose intensity values fill in that particular bin. The histogram can be described as:

$H = \{ h(i) \mid i = 1,2,3….256 \mid \}$

	
(a)Cover “dollar.bmp” image	(e)Watermarked “dollar.bmp” image



(b)Cover "lighthouse.png" image

(f)Watermarked "lighthouse.png" image

(c)Cover"woman.tif" image

(g)Watermarked "woman.tif" image

(d) Cover "lena.gif" image

(h)Watermarked "lena.gif" image

Fig 6. Histograms of the cover images and their corresponding watermarked images

Figure 6. (e) - (h) shows the histogram stretching method called as histogram equalization that exhibits a rather uniform distribution of its pixel values. It returns the enhanced contrast gray scale transformation that maps gray levels in the input image to gray levels in output image. The changed locations in histograms can be observed in the adjacent pixels whose differences are larger a lot. The extent of this change depends on the embedded watermark and pixel size. The histogram shows the uniform distribution of the watermark pixel values over the whole cover image. They cover a broad portion of the allowed range thereby depicting the robustness of the watermark.

Computational Complexity – It refers to the time taken by a method to embed the watermark image into the cover image.

Table 9. Elapsed Time taken by different images

Cover Image	Elapsed Time (sec)
Image 1	2.2188
Image 2	2.2813
Image 3	2.3906
Image 4	1.3438

Table 9 Shows the elapsed time or processing time of the CPU, in seconds, to embed the watermark in the cover image. Thus it can be observed that the time taken for the computation is much smaller as the SVD is applied only to a 64x64 matrix of a 512x512 grayscale cover image and does not affect much with the change in the image file formats.The chapter discussed the conducted experiments and evaluates the results based on different evaluation parameters. The performance analysis is carried out by keeping in view the various factors significant for the watermarking method. Various formulae, figures, tables and graphs illustrate the imperceptibility and robustness of the method against various types of attacks esp. the JPEG compression and histogram equalization. The method shows the optimal amount of time complexity with different kind of images that shows the varied applicability of the method.

VI CONCLUSION

Watermarking is the process of embedding information into the multimedia content to prove the "ownership" authentication so that the quality degradation is minimized and imperceptible level is maintained. The proposed algorithm mainly focuses on gray scale digital images using the wavelet and singular domain with different dual scrambling methodology to increase the robustness of the watermarked image against certain types of noise and attacks. Different degree and key values are presented that can be used according to the application area.

VII SCOPE FOR FUTURE ENHANCEMENTS

The proposed algorithm can be further extended to the 3-D RGB colored images where watermarking can be done at each plane thereby increasing the hiding capacity of images without much altering the imperceptibility parameter. The other future scope is that the method can be combined with some Visual Cryptographic (VC) methods along with the encryption and decryption at different levels to further enhance the security of watermarks. Further, research is needed to make it work in the audio and video systems.

REFERENCES

[1] Wang, Ben, Ding, Jinkou, Wen, Qiaoyan, Liao, Xin, Liu, Cuixiang. 2009. An Image Watermarking Algorithm Based on DWT

DCT and SVD. Proceeding IC-NIDC, 1034-1037.

[2] Rui-mei, Zhao, Mei, Wang, Bo-ning Hu and Hua, Lian. 2010. Digital Image Watermarking Algorithm Based on Wavelet Transform. Third International Symposium on Intelligent Information Technology Application, 2: 437:440.

[3] Singh, Dharm, Choudhary, Naveen and Agrawal, Madhuri.2012. Spatial and Frequency Domain for Grey level Digital Images. IJCA Special Issue on Communication Security (comnetcs), 16-20.

[4] Gunjal, B.L. and Manthalkar, R.R. 2010. Discrete Wavelet Transform based Strongly Robust Watermarking Scheme for Information Hiding in Digital Images. IEEE 3rd International Conference on Emerging Trends in Engineering and Technology, 124 – 129.